98TH CONGRESS } HOUSE OF REPRESENTATIVES { REPT. 98–
1st Session } { 423 Part 1

SMALL BUSINESS COMPUTER CRIME PREVENTION ACT

OCTOBER 20, 1983.—Ordered to be printed

Mr. MITCHELL, from the Committee on Small Business, submitted the following

REPORT

[To accompany H.R. 3075 which on May 19, 1983, was jointly referred to the Committee on Small Business and the Committee on the Judiciary]

[Including cost estimate of the Congressional Budget Office]

The Committee on Small Business, to whom was referred the bill (H.R. 3075) to amend the Small Business Act to establish a Small Business Computer Crime and Security Task Force, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SHORT TITLE

SECTION 1. This Act may be cited as the "Small Business Computer Crime Prevention Act".

FINDINGS AND PURPOSES

SEC. 2. (a) The Congress hereby finds that—

(1) there is an increased dependency on, and proliferation of, information technology (including computers, data networks, and other communication devices) in the small business community;

(2) such technology has permitted and expanded criminal activity against small business concerns; and

(3) small business concerns are not always able to protect their information technology from computer criminals.

(b) The purposes of this Act are—

(1) to improve the management by small business concerns of their information technology; and

(2) to encourage small business concerns to protect such technology from criminal activity.

COMPUTER CRIME AND SECURITY TASK FORCE

SEC. 3. Section 4(b) of the Small Business Act (15 U.S.C. 633(b)) is amended by adding at the end thereof the following new paragraph:

"(3)(A) The Administrator shall, not later than 60 days after the effective date of this paragraph, establish a task force to be known as the 'Small Business Computer Crime and Security Task Force'.

31-006 O

H723-7

"(B) The Task Force shall consist of the following members:

"(i) an employee of the Small Business Administration, appointed by the Administrator;

"(ii) an employee of the Institute for Computer Sciences and Technology of the Department of Commerce, appointed by the Secretary of Commerce;

"(iii) an employee of the Department of Justice, appointed by the Attorney General;

"(iv) an employee of the Department of Defense, appointed by the Secretary of Defense;

"(v) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer hardware to small business concerns;

"(vi) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer software to small business concerns;

"(vii) one individual, appointed by the Administrator, who is representative of the interests of the providers of insurance to small business concerns;

"(viii) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer security equipment and services to small business concerns;

"(ix) one individual, appointed by the Administrator, who is representative of the interests of associations of small business concerns, other than small business concerns engaging in any of the activities described in clauses (v) through (viii); and

"(x) such additional qualified individuals, appointed by the Administrator, as the Administrator determines to be appropriate.

"(C) It shall be the function of the Task Force—

"(i) to define the nature and scope of computer crimes committed against small business concerns;

"(ii) to ascertain the effectiveness of State legislation, and available security equipment, in preventing computer crimes against small business concerns;

"(iii) in cooperation with the National Bureau of Standards, to develop guidelines to assist small business concerns in evaluating the security of computer systems; and

"(vi) to make recommendations to the Administrator with respect to the appropriate activities of the resource center established under paragraph (4).

"(D) The Administrator shall designate one of the members of the Task Force as its chairperson. The Task Force shall meet not less than once during 6-month period following the effective date of this paragraph, at the call of its chairperson. A majority of the members of the Task Force shall constitute a quorum.

"(E) Each member of the Task Force shall serve without additional pay, allowances, or benefits by reason of such service. To the extent and in the amounts provided in advance in appropriations Acts, each such member shall be reimbursed for actual expenses, including travel expenses, determined by the Administrator to have been reasonably incurred in the course of performing the functions vested in the Task Force.

"(F) The Administrator shall provide the Task Force with such staff and office facilities as the Administrator, following consultation with the Task Force, considers necessary to permit the Task Force to carry out its functions under this paragraph.

"(G) The Task Force may secure directly from any Federal agency information necessary to enable the Task Force to carry out its functions under this paragraph. Upon request of the chairperson of the Task Force, the head of such agency shall furnish such information to the Task Force.

"(H) Not later than 18 months after the effective date of this paragraph, the Task Force shall submit to the President, the Administrator, and the Congress a detailed report setting forth the findings of the Task Force with respect to the matters described in subparagraph (C) and containing such recommendations as the Task Force determines to be appropriate.

"(I) The Task Force shall terminate not later than 30 days after the submission of its report under subparagraph (H).

"(J) For purposes of this paragraph and paragraph (4)—
"(i) the term 'computer crime' means—
"(I) any crime committed against a small business concern by means of the use of a computer; and
"(II) any crime involving the illegal use of, or tampering with, a computer owned or utilized by a small business concern; and
"(ii) the term 'Task Force' means the Small Business Computer Crime and Security Task Force established under subparagraph (A).".

COMPUTER CRIME AND SECURITY INFORMATION

SEC. 4. Section 4(b) of the Small Business Act (15 U.S.C. 633(b)), as amended in section 3 of this Act, is amended by adding at the end thereof the following new paragraph:
"(4)(A) The Administrator shall—
"(i) provide to small business concerns information regarding—
"(I) computer crimes committed against small business concerns; and
"(II) security for computers owned or utilized by small business concerns; and
"(ii) provide for periodic regional forums for small business concerns to improve the exchange of information regarding the matters described in clause (i).
"(B) Not later than 60 days after receipt of the report of the Task Force under paragraph (3)(H), the Administrator shall establish as part of the Small Business Administration a resource center that will carry out the functions of the Administrator under subparagraph (A)(i).".

THE PURPOSE OF THE BILL

The purpose of the bill is to provide small businesses with information to help improve the management of their information technology, and to protect such technology from the criminal activity.

INTRODUCTION AND BACKGROUND

The use of computers by business has expanded rapidly over the last decade. As the cost and size of computer systems has diminished, their use by small business has multiplied. Along with the increased use of information systems has come the increased abuse of the new technology for criminal purposes. Small businesses are particularly vulnerable to computer crimes because of a lack of resources, skills and information necessary to adequately protect their system from computer criminals

H.R. 3075, introduced by Mr. Wyden on May 19, 1983, is designed to provide small businesses with the information necessary to evaluate and improve their computer security.

Your Subcommittee on Antitrust and Restraint of Trade Activities Affecting Small Business held a hearing on the legislation on July 14, 1983, in Washington, D.C. Testifying in support of the bill were a representative of the computer software industry, a law enforcement official, authorities on computer crime, and a small businessman whose business had been victimized by a computer crime.

The legislation was considered by the Subcommittee on September 15, 1983. An amendment in the nature of a substitute, offered by Mr. Luken, was accepted by unanimous voice vote. The amendment incorporated several cost saving changes suggested by witnesses at the hearing and through informal discussions by the Members. No additional

amendments were offered, and the bill was reported as amended to the full committee by unanimous voice vote.

As the use of computers has grown, so has the incidence of computer crime. Estimates of the losses in the private sector are as high as $1 billion annually, although accurately estimating losses is nearly impossible for several reasons. Victims are often reluctant to report crimes for fear of bad publicity. Also, computer crime statistics are reported, not as "computer crimes", but as ordinary white-collar crime (fraud, theft, embezzlement, etc.) This makes compilation of accurate computer crime statistics a very difficult, if not impossible, task.

Often, computer crimes are new ways of committing old crimes. Some of the more common types of computer crime are: theft of merchandise or property through the use of a computer, unauthorized use of someone else's computer, the theft, copyright infringement, or unauthorized destruction or alteration of computer stored information or programs, and financial crimes such as directing payments to phony suppliers or employees.

Your Subcommittee heard about one incident in which a family money order business lost over $100,000 because an employee was able to use his knowledge of computers to create and cash phony money orders.

Small businesses are often more vulnerable to computer crimes than large businesses. Large businesses can have elaborate security procedures, and extensive internal and external auditing. Thus, computer crimes can often be detected relatively quickly. Quick detecting, together with contingency planning and good insurance, keep the cost of computer crime for large businesses relatively low.

Small businesses suffer from a number of disadvantages. They often lack the resources, or do not recognize the need for implementing computer security safeguards. They often cannot afford to hire security consultants. In addition, small businesses lack the in-house expertise to investigate computer crimes. Management may also lack the expertise to properly oversee a company's computer operations, thereby giving the programmer or operator a virtual free-hand. Some salesmen may not inform customers of the vulnerabilities of their computer related products in an effort to present those products in a favorable light.

After a computer crime is committed, the small businessman may not be able to rely on the criminal justice system for help. Law enforcement agencies at all levels are unprepared to meet the challenge of the computer crime problem. The judicial system is equally unprepared for this challenge. Law enforcement officials encourage the preventive approach which costs far less than the long investigation, complex prosecution, and incarceration involved in a successfully prosecuted case.

However, most computer crimes never reach the prosecution state. Crimes using computers are among the most difficult to detect, and many of these crimes go undiscovered.

Two forces are emerging to encourage small business owners to pay closer attention to computer security concerns. The first is the insurance industry, which is starting to vary premiums based on the amount of the insured's computer security, and the second is the growing computer security products industry. Current government research on computer security is directed primarily towards federal agencies. The

Task Force computer security guidelines, and the SBA sponsored forums and resource center called for in H.R. 3075 are designed to both educate and increase the awareness of the small businessperson to computer security problems.

What the Bill Would Do

The bill, H.R. 3075, contains Congressional findings that there is an increased dependency on information technology, including computers, in the small business community; that such technology has permitted and expanded criminal activity against small businesses; and that small businesses are not always able to protect their information technology from computer crime.

The bill's stated purposes are to improve small businesses management of their information technology and protect it from criminal activity.

I. ESTABLISHMENT OF TASK FORCE

The bill would direct the Administrator of the Small Business Administration, within sixty days, to establish a "Small Business Computer Crime and Security Task Force". The Task Force would consist of an employee of each of the following four departments who would be named by the Department head: the Small Business Administration, the Institute for Computer Sciences and Technology of the Department of Commerce, the Department of Justice and the Department of Defense; it would also consist of five other members, appointed by the Administrator of SBA, and who would be representative of each of the following groups: the providers of computer hardware to small business, the providers of computer software to small business, the providers of insurance to small business, the providers of computer security equipment and services to small business, and the general associations of small business concerns. In addition, the Administrator would be authorized to appoint such other members to the Task Force as he deemed appropriate.

II. FUNCTION OF TASK FORCE

The function of the Task Force would be to define the nature and scope of computer crimes committed against small business; to ascertain the effectiveness of state legislation and available security equipment in preventing computer crimes against small businesses; in cooperation with the National Bureau of Standards, to develop guidelines to assist small businesses in evaluating the security of computer systems; and to recommend to the Administrator appropriate activities of an on-oing resource center to assist small business in combatting computer crime.

Within eighteen months, the Task Force would submit a report to the President, the Administrator and the Congress, and would cease to exist thirty days after submission of the report.

III. RESOURCE CENTER

Not later than sixty days of receipt of the Task Force report, the Administrator of the SBA would be required to establish a Resource Center which would provide to small businesses information regarding

computer crimes and security for computers. The Administrator would also be directed to provide for periodic regional forums for small businesses to improve the exchange of information regarding these matters.

Your committee intends that the SBA will utilize its current resources to immediately make available computer security information to small businesses while awaiting the report of the Task Force.

IV. CONCLUSION

Your committee believes that the bill, H.R. 3075, the Small Business Computer Crime Prevention Act, is an inexpensive, common sense response to the growing problem of computer crime against small business.

This bill will enable small concerns to better evaluate the security of their computer systems so that the losses due to crimes committed by computer can be minimized.

Matters Required To Be Discussed Under House Rules

In compliance with clause 2(l)(2) of rule XI of the House of Representatives, the following statement is made relative to the vote on the motion to report H.R. 3075:

A majority of the committee voted in person and was actually present and the motion was approved by a recorded vote of 30 ayes and no nays.

In compliance with clause 2(l)(3) of rule XI of the Rules of the House of Representatives, the following statements are made:

With regard to subdivision (A), relating to oversight findings, the committee finds, in keeping with clause 2(b)(1) of rule X, that this legislation is in full compliance with the provision of this rule of the House which states:

> In addition, each such committee shall review and study any conditions or circumferences which may indicate the necessity or desirability of enacting new or additional legislation within the jurisdiction of that committee. * * *

With regard to subdivision (B), relating to the statement required by section 308(a) of the Congressional Budget Act of 1974, the following statement is made relative to the legislation:

> Section 3(a)(2) of the Congressional Budget Act defines the term "tax expenditures" as those revenue losses attributable to provisions of the Federal tax laws which allow a special exclusion, exemption, or deduction, from gross income or which provide a special credit, a preferential rate of tax, or a deferral of tax liability.

None of the provisions of H.R. 3075 deals with taxation and thus, in your committee's opinion, this bill does not provide new or increased tax expenditures.

Section 3(a)(2) of the Congressional Budget Act defined the term "budget authority" as authority provided by law to enter into obligations which will result in immediate or future outlays involving Government funds.

Under this definition, it is the final action of Congress that authorizes an agency to enter into obligations which constitutes new budget authority. In those cases which entail (1) an authorization for an agency to undertake a program; (2) an authorization for appropriation of funds to permit that agency to enter into obligations; and (3) an actual appropriation of such funds, it would be only the final action of Congress in appropriating funds which constitutes the budget authority.

None of the provisions of H.R. 3075 appropriates funds and thus, in your committee's opinion, the bill does not provide new budget authority. Accordingly, no comparison of budget authority, outlays or tax expenditures or 5-year projections have been made.

With regard to subdivisions (C) and (D), the cost estimate of the Director of the Congressional Budget Office relative to H.R. 3075 follows:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, D.C., October 13, 1983.

Hon. PARREN J. MITCHELL,
Chairman, Committee on Small Business, U.S. House of Representatives, Washington, D.C.

DEAR MR. CHAIRMAN: Pursuant to Section 403 of the Congressional Budget Act of 1974, the Congressional Budget Office has reviewed H.R. 3075, the Small Business Computer Crime Prevention Act, as ordered reported by the House Committee on Small Business, October 4, 1983.

H.R. 3075 would establish a Small Business Computer Crime and Security Task Force, composed of representatives from the federal government and the private sector. The task force, under the direction of the Administrator of the Small Business Administration (SBA), would be required to report within 18 months to the President and the Congress regarding its findings and recommendations on computer crimes and security. The SBA would be required to provide necessary support staff and office facilities. Task force members would serve without pay, but would be reimbursed for actual expenses, including travel. Based on information provided by the SBA, and assuming a date of enactment around January 1, 1984, it is estimated that the cost of the task force would be approximately $60,000 in each of the fiscal years 1984 and 1985. The estimated cost could be somewhat more or less, depending upon the number and location of meetings, as well as the scope of the annual report.

In addition, H.R. 3075 would require the SBA, upon completion of the report of the task force, to establish a resource center within SBA to provide small businesses information regarding computer crimes and safety. Although the organizational structure of the proposed resource center is not clear at this time, according to information from the SBA it is expected that approximately $100,000 annually, beginning in fiscal year 1986, would be required to implement this provision.

Enactment of this bill would not affect the budget of state and local governments.

Should the Committee so desire, we would be pleased to provide further details on this estimate.

Sincerely,

RUDOLPH G. PENNER,
Director.

No oversight findings or recommendations have been made by the Committee on Government Operations with respect to the subject matter contained in H.R. 3075.

In compliance with clause 2(l)(4) the committee concludes that the provisions of this legislation in and of themselves will have no inflationary impact on prices and costs in the operation of the national economy.

In compliance with clause 7, rule XIII of the House of Representatives, the committee makes the following statement:

The costs attributable to this bill for the current fiscal year and for fiscal years 1985–89 are as follows: It is expected that the Task Force will exist for two years at a cost of some $60,000 per year. At that time, the on-going costs are estimated at some $100,000 per year to disseminate information to the small business community. Thus, the committee estimates the cost of the bill at approximately $500,000. No new or additional authorization or appropriation is being provided and it is fully expected that the costs will be paid from the SBA's overall budget.

No cost estimate was submitted by any Government agency on H.R. 3075 to your committee.

In your committee's opinion, the above statements fully comply with the Rules of the House of Representatives.

SECTION-BY-SECTION ANALYSIS

Section 1 provides that this Act may be cited as the "Small Business Computer Crime Prevention Act".

Section 2(a) includes Congressional findings that:

(1) there is an increased dependency on, and proliferation of, information technology (including computers, data networks, and other communication devices) in the small business community;

(2) such technology has permitted and expanded criminal activity against small business concerns; and

(3) small business concerns are not always able to protect their information technology from computer criminals.

Section 2(b) states that the purposes of the Act are:

(1) to improve the management by small business concerns of their information technology; and

(2) to encourage small business concerns to protect such technology from criminal activity.

Section 3 amends section 4(b) of the Small Business Act by adding a new paragraph requiring the Administrator of SBA, within sixty days, to establish a Task Force to be known as the "Small Business Computer Crime and Security Task Force."

The new section 4(b)(3)(B) would designate membership on the Task Force as follows:

(i) an employee of the Small Business Administration, appointed by the Administrator;

(ii) an employee of the Institute for Computer Sciences and Technology of the Department of Commerce, appointed by the Secretary of Commerce;

(iii) an employee of the Department of Justice, appointed by the Attorney General;

(iv) an employee of the Department of Defense, appointed by the Secretary of Defense;

(v) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer hardware to small business concerns;

(vi) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer software to small business concerns;

(vii) one individual, appointed by the Administrator, who is representative of the interests of the providers of insurance to small business concerns;

(viii) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer security equipment and services to small business concerns;

(ix) one individual, appointed by the Administrator, who is representative of the interests of the associations of small business concerns, other than small business concerns engaging in any of the activities described in clauses (v) through (viii); and

(x) such additional qualified individuals, appointed by the Administrator, as the Administrator determines to be appropriate.

The new 4(b)(3)(C) would provide that it is the function of the Task Force:

(i) to define the nature and scope of computer crimes committed against small business concerns;

(ii) to ascertain the effectiveness of State legislation, and available security equipment, in preventing computer crimes against small business concerns;

(iii) in cooperation with the National Bureau of Standards, to develop guidelines to assist small business concerns in evaluating the security of computer systems; and

(iv) to make recommendations to the Administrator with respect to the appropriate activities of the resource center established under paragraph (4).

The new 4(b)(3)(D) requires the Administrator to designate one of the members of the Task Force as its chairperson. The Task Force would be required to meet not less than once during every six-month period, at the call of the chairperson, with a majority of the members constituting a quorum.

The new 4(b)(3)(E) provides the Task Force members will serve without additional pay, but would be reimbursed for actual expenses reasonably incurred.

The new 4(b)(3)(F) requires the Administrator to provide the Task Force with staff and office facilities.

The new 4(b)(3)(G) authorizes the Task Force to secure information from any Federal agency.

The new 4(b)(3)(H) requires the Task Force, within eighteen months, to submit to the President, the Administrator and the Congress a detailed report on the findings of the Task Force as described in the new subparagraph (C) and such recommendations as it determines to be appropriate.

The new 4(b)(3)(I) terminates the Task Force not later than thirty days after submission of its report.

The new 4(b)(3)(J) contains definitions as follows:

(i) the term "computer crime" means—

(I) any crime committed against a small business concern by means of the use of a computer; and

(II) any crime involving the illegal use of, or tampering with, a computer owned or utilized by a small business concern; and

(ii) the term "Task Force" means the Small Business Computer Crime and Security Task Force established under subparagraph (A).

Section 4 further amends section 4(b) of the Small Business Act by adding a new paragraph (4)(A) which requires the Administrator of SBA to:

(i) provide to small business concerns information regarding: (I) computer crimes committed against small business concerns; and (II) security for computers owned or utilized by small business concerns; and

(ii) provide for periodic regional forums for small business concerns to improve the exchange of information regarding the matters described in clause (i).

The new Section 4(b)(4)(B) requires the Administrator, within sixty days after receipt of the Task Force report, to establish a Resource Center that will carry out the functions of the Administrator under section 4(b)(4)(A)(i).

Changes in Existing Law Made by the Bill, As Reported

In compliance with clause 3 of Rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italic, existing law in which no change is proposed is shown in roman):

Section 4 of the Small Business Act

Sec. 4. (a) In order to carry out the policies of this Act there is hereby created an agency under the name "Small Business Administration" (herein referred to as the Administration), which Administration shall be under the general direction and supervision of the President and shall not be affiliated with or be within any other agency or department of the Federal Government. The principal office of the Administration shall be located in the District of Columbia. The Administration may establish such branch and regional offices in other places in the United States as may be determined by the Administrator of the Administration. As used in this Act, the term "United States" includes the several States, the Territories and possessions of the United States, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and the District of Columbia.

(b)(1) The management of the Administration shall be vested in an Administrator who shall be appointed from civilian life by the President, by and with the advice and consent of the Senate, and who shall be a person of outstanding qualifications known to be familiar and sympathetic with small-business needs and problems. The Administrator shall not engage in any other business, vocation, or employment than that of serving as Administrator. In carrying out the programs administered by the Small Business Administration including its lending and guaranteeing functions, the Administrator shall not discriminate on the basis of sex or marital status against any person or small business concern applying for or receiving assistance from the Small Business Administration, and the Small Business Administration shall give special consideration to veterans of the Armed Forces of the United States and their survivors or dependents. The Administration is authorized to appoint a Deputy Administrator and four Associate Administrators (including the Associate Administrator specified in section 201 of the Small Business Investment Act of 1958) to assist in the execution of the functions vested in the Administration.[1] One of the Associate Administrators shall be designated at the time of his appointment as the Associate Administrator for Minority Small Business and Capitol Ownership Development and shall be responsible to the Administrator for the formulation and execution of the policies and programs under sections 7(j) and 8(a) of this Act which provide assistance to minority small business concerns.

(2) The Administrator also shall be responsible for—

(A) establishing and maintaining an external small business economic data base for the purpose of providing the Congress and the Administration information on the economic condition and the expansion or contraction of the small business sector. To that end, the Administrator shall publish on a regular basis national small business economic indices and, to the extent feasible, regional small business economic indices, which shall include, but need not be limited to, data on—

(i) employment, layoffs, and new hires;

(ii) number of business establishments and the types of such establishments such as sole proprietorships, corporations, and partnerships;

(iii) number of business formations and failures;

(iv) sales and new orders;

(v) back orders;

(vi) investment in plant and equipment;

(vii) changes in inventory and rate of inventory turnover;

(viii) sources and amounts of capital investment, including debt, equity, and internally generated funds;

(ix) debt to equity ratios;

(x) exports;

(xi) number and dollar amount of mergers and acquisitions by size of acquiring and acquired firm; and

(xii) concentration ratios; and

(B) publishing annually a report giving a comparative analysis and interpretation of the historical trends of the small business sector as reflected by the data acquired pursuant to subparagraph (A) of this subsection.

(3)(A) The Administrator shall, not later than 60 days after the effective date of this paragraph, establish a task force to be known as the "Small Business Computer Crime and Security Task Force".

(B) The Task Force shall consist of the following members:

(i) an employee of the Small Business Administration, appointed by the Administrator;

(ii) an employee of the Institute for Computer Sciences and Technology of the Department of Commerce, appointed by the Secretary of Commerce;

(iii) an employee of the Department of Justice, appointed by the Attorney General;

(iv) an employee of the Department of Defense, appointed by the Secretary of Defense;

(v) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer hardware to small business concerns;

(vi) one individual appointed, by the Administrator, who is representative of the interests of the providers of computer software to small business concerns;

(vii) one individual, appointed by the Administrator, who is representative of the interests of the providers of insurance to small business concerns;

(viii) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer security equipment and services to small business concerns;

(ix) one individual, appointed by the Administrator, who is representative of the interests of associations of small business concerns, other than small business concerns engaging in any of the activities described in clauses (v) through (viii); and

(x) such additional qualified individuals, appointed by the Administrator, as the Administrator determines to be appropriate.

(C) It shall be the function of the Task Force—

(i) to define the nature and scope of computer crimes committed against small business concerns;

(ii) to ascertain the effectiveness of State legislation, and available security equipment, in preventing computer crimes against small business concerns;

(iii) in cooperation with the National Bureau of Standards, to develop guidelines to assist small business concerns in evaluating the security of computer systems; and

(iv) to make recommendations to the Administrator with respect to the appropriate activities of the resource center established under paragraph (4).

(D) The Administrator shall designate one of the members of the Task Force as its chairperson. The Task Force shall meet not less than once during each 6-month period following the effective date of this paragraph, at the call of its chairperson. A majority of the members of the Task Force shall constitute a quorum.

(E) Each member of the Task Force shall serve without additional pay, allowances, or benefits by reason of such service. To the extent and in the amounts provided in advance in appropriations Acts, each such member shall be reimbursed for actual expenses, including travel

expenses, determined by the Administrator to have been reasonably incurred in the course of performing the functions vested in the Task Force.

(F) The Administrator shall provide the Task Force with such staff and office facilities as the Administrator, following consultation with the Task Force, considers necessary to permit the Task Force to carry out its functions under this paragraph.

(G) The Task Force may secure directly from any Federal agency information necessary to enable the Task Force to carry out its functions under this paragraph. Upon request of the chairperson of the Task Force, the head of such agency shall furnish such information to the Task Force.

(H) Not later than 18 months after the effective date of this paragraph, the Task Force shall submit to the President, the Administrator, and the Congress a detailed report setting forth the findings of the Task Force with respect to the matters described in subparagraph (C) and containing such recommendations as the Task Force determines to be appropriate.

(I) The Task Force shall terminate not later than 30 days after the submission of its report under subparagraph (H).

(J) For purposes of this paragraph and paragraph (4)—

(i) the term "computer crime" means—

(I) any crime committed against a small business concern by means of the use of a computer; and

(II) any crime involving the illegal use of, or tampering with, a computer owned or utilized by a small business concern; and

(ii) the term "Task Force" means the Small Business Computer Crime and Security Task Force established under subparagraph (A).

(4)(A) The Administrator shall—

(i) provide to small business concerns information regarding—

(I) computer crimes committed against small business concerns; and

(II) security for computers owned or utilized by small business concerns; and

(ii) provide for periodic regional forums for small business concerns to improve the exchange of information regarding the matters described in clause (i).

(B) Not later than 60 days after receipt of the report of the Task Force under paragraph (3)(H), the Administrator shall establish as part of the Small Business Administration a resource center that will carry out the functions of the Administrator under subparagraph (A)(i).

* * * * * * *

○